(19) **KOREAN INTELLECTUAL PROPERTY OFFICE**

KOREAN PATENT ABSTRACTS

(11)Publication number: **1020010073358 A**

(43)Date of publication of application: **01.08.2001**

(21)Application number: **1020000001699**

(22)Date of filing: **14.01.2000**

(30)Priority: **..**

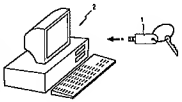
(51)Int. Cl **G06F 11/00**

(71)Applicant: **LEE, KI RYOUNG**

(72)Inventor: **BANG, SANG UNG**
KWON, O SIN
LEE, KI RYOUNG
MA, JEONG U
PARK, JE BEOM
SEO, JUN WON

(54) **SYSTEM FOR SECURING SECRET KEY BY USING USB PORT**

(57) Abstract:



PURPOSE: A secret key securing system is provided to prevent a physical access to a secret key in a memory when a user is robbed of a secret key storage and coding/decoding device by generating coding/decoding data without an exposure of the secret key. CONSTITUTION: The system comprises a power supply terminal, a power on/off switch, a ROM, and a data I/O terminal. The power supply terminal receives electric power from a computer as soon as it is inserted into a USB(Universal Serial Bus) port of the computer. The power on/off switch mechanically switches on or off the electric power supplied by the power supply terminal. The ROM is enabled and then generates secret key data of a user if the user switches on the power on/off switch. The data I/O terminal transmits the secret key data to the USB port. The secret key data is a private key distributed for a specific user for a user certification or data security by a specific organization or an electronic signature key data issued by the CA(Certificate Authority).

Legal Status

Date of request for an examination (20000114)
Notification date of refusal decision ( )
Final disposal of an application (registration)
Date of final disposal of an application (20020131)
Patent registration number (1003326900000)
Date of registration (20020402)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl. 7
G06F 11/00

(45) 공고일자 2002년04월15일
(11) 등록번호 10 -0332690
(24) 등록일자 2002년04월02일

(21) 출원번호 10 -2000 -0001699
(22) 출원일자 2000년01월14일

(65) 공개번호 특2001 -0073358
(43) 공개일자 2001년08월01일

(73) 특허권자 이기룡
서울 서초구 반포동 주공3단지아파트 337동 401호

(72) 발명자 이기룡
서울 서초구 반포동 주공3단지아파트 337동 401호
방상웅
서울특별시노원구상계3동대림APT106 -507
마정우
경기도광주군오포면추자리507 -5낙원타운2동
서준원
서울특별시성북구정릉4동266 -54335/9
권오신
경기도용인시기흥읍고매리세원APT101 -608
박제범
서울특별시송파구삼전동113 -4

(74) 대리인 이화익

심사관 : 류동현

(54) 유.에스.비 포트 방식의 비밀키 보안장치

요약

본 발명은 USB(Universal Serial Bus) 포트 방식의 비밀키 보안장치에 관한 것이다. 본 비밀키 보안장치(30)는, 열쇠처럼 만들어져서, 전원이 온(ON) 된 상태의 컴퓨터(2)에 내장된 USB 포트(3)에 삽입한다. 이에 따라 컴퓨터로부터 전원전송단자(31)를 통해 전원이 전송되고, 사용자가 전원 공급/차단 스위치(32)를 기계적인 조작으로 온(on) 시켜 영구 메모리(35)가 인에이블 상태로 되면서, 영구 메모리에 저장되어 있던 비밀키가 데이터 입출력단자(38)를 통해 USB 포트(3)에 전송된다. 본 발명의 다른 실시예로서, 상기 전원공급/차단 스위치의 온(on)조작으로 전원이 임시메모리(35), 영구 메모리(36), 암호/복호 프로세서(37)에 공급되고, 이에 따라 사용자가 암호/복호 선택 스위치(34)를 선택하면 그 선택된 신호에 따라 데이터 입출력단자를 통하여 암호화할 또는 암호화된 데이터가 입력되어 그 임시메모리에 저장되고, 그 임시 메모리에 저장된 데이터를 영구메모리에 저장된 비밀키(암호키 또는 복호키)를 사용하여 프로세

서가 전자서명에 필요한 암호 데이터(전자서명) 또는 복호 데이터로 생성하여 임시메모리에 저장한 후, 데이터 입출력단자를 통해 USB 포트에 전송하는 구성으로 이루어진다. 또한 지문인식기(33)를 추가하여 사전에 사용자 검증을 할 수가 있다. 이러한 본 발명은 기계적 전원 공급/차단 스위치를 통하여 소프트웨어적으로 비밀키 저장장치를 해킹하려는 접근차단과 암호/복호 프로세서를 통하여 소프트웨어적으로 컴퓨터를 해킹하려는 접근차단으로부터 비밀키의 안전성, 비밀성을 보장하며, 지문인식기를 통하여 물리적 접근 통제의 효과가 있다.

대표도
도 5

명세서

도면의 간단한 설명

도 1은 일반적인 전자서명의 개념도,

도 2는 종래 USB 포트방식의 비밀키 저장장치가 적용되는 개념도,

도 3은 본 발명의 제 1 실시예에 따른 비밀키 보안장치의 블록 구성도,

도 4는 본 발명의 제 2 실시예에 따른 비밀키 보안장치의 블록 구성도,

도 5는 본 발명의 제 3 실시예에 따른 비밀키 보안장치의 블록 구성도.

*도면의 주요 부분에 대한 부호의 설명

1 : USB 포트방식의 비밀키 저장장치(iKey)

2 : USB 포트가 설치된 컴퓨터 3 : USB 포트

10, 20, 30 : USB 포트 방식의 비밀키 보안장치

11, 22, 31 : 전원전송단자 12, 23, 32 : 전원 공급/차단 스위치

13, 25, 36 : 영구 메모리 14, 27, 38 : 데이터 입출력단자

21, 34 : 암호/복호 선택 스위치 24, 35 : 임시 메모리

26, 37 : 암호/복호 프로세서 33 : 지문 인식기

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 컴퓨터에 내장된 USB(Universal Serial Port) 포트에 연결시켜서 비밀키(암호키, 복호키)의 비밀성 보장을 위한 USB 포트 방식의 비밀키 보안장치에 관한 것이다.

최근, 인터넷의 급성장으로 인해 전자상거래, 전자화폐, 가상은행과 같은 새로운 정보화 시대의 출현을 초래하였다. 더욱이 정보가 디지털화됨에 따라 고성능의 컴퓨팅 기술과 고속의 네트워크를 통하여 고집적화 및 고속전송이 되면서 정보가 간단한 컴퓨터 조작만으로도 손쉽게 복제, 침해, 도용, 남용될 가능성이 폭증하고 있다.

정보보호의 방법으로 정보의 암호화, 복호화 기술이 발전하고 있으며, 그 구현 방법으로 암호화 및 복호화에 같은 키를 사용하는 대칭키 암호 시스템, 키 공유, 분배 문제를 해결하기 위하여 암호키와 복호키가 서로 다른 공개키 암호 시스템이 있다. 키의 분배가 쉽고 복호키를 알고 있어도 암호키를 알아내는 것이 계산상 불가능(computational infeasible)한 공개키 암호 시스템을 기반으로 하는 많은 연구가 진척되었다.

이러한 암호기법의 발전으로 전자상거래, 전자화폐, 가상은행과 같은 디지털 기반에서 사용자 인증, 부인방지, 변경불가, 재사용불가, 위조불가의 특성을 제공하는 '전자서명'방법이 필요하고, 법률 제5,792호(1999. 2. 5) '전자서명법' 및 대통령령 제16,457호(1999.6.30) '전자서명법시행령'으로 공개키 암호 시스템 기반의 전자서명법이 1999년 7월 1일부로 시행되었으며, 정보통신부 장관이 지정한 공인인증기관에서 보관, 배포하는 전자서명검증키(공개되어 있는 복호키)와 디스켓, 컴퓨터, 스마트 카드에 전자서명생성키(비공개되어 있는 암호키)를 저장하는 방법을 사용하고 있다.

위에서, 전자서명이란, 도 1에 도시된 바와 같이, 사용자가 전자서명생성키 와 인증서를 인증센터로부터 발급 받아 디지털 데이터에 대한 사용자 인증이 필요할 때 자신의 전자서명 생성키 (비공개 암호키)로 해당 데이터를 암호화하여 전자서명을 생성한 다음 사용자인증 요구자에게 해당 데이터와 전자서명 그리고 인증서를 전송한다. 요구자는 인증서를 인증센터에 의뢰하여 해당 사용자의 인증서 임을 확인하고 공개되어 있는 인증자의 전자서명검증키(공개되어 있는 복호키)로 전자서명을 복호하여 원래 데이터와 비교하여 동일함을 확인함으로서 해당 사용자가 전송한 데이터가 변경되지 않았으며 전송자의 신원이 확실함을 확인할 수 있다.

하지만 상기 비밀키 저장장치를 사용하였을 경우 안전성과 사용의 문제점이 있다. 비밀키를 플로피디스크 혹은 하드디스크에 저장하여 사용할 경우 타인의 복제가 쉽고 이를 보안하기 위한 스마트 카드의 사용에 있어서는 스마트 카드 리더기를 설치해야 하는 비용과 범용성에 문제가 있다. 이러한 문제를 해결하기 위한 방법으로 래인보우 테크놀로지사에서는 USB포트 방식의 비밀키 저장장치를 발표하였다.

USB(Universal Serial Bus)란 인텔, 컴팩, IBM, DEC, 마이크로소프트, NEC, 노던텔레콤 등 7개 기업이 합의한 PC 주변기기 포트규격으로 PC의 표준포트로 자리잡았다. 이러한 USB 포트는 초당 최대 12 MByte의 고속으로 데이터를 전송할 수 있고, 또한 최대 127개까지의 주변장치를 연결할 수 있는 확장성도 뛰어나다. 아울러, 주변장치를 추가 설치할 때 컴퓨터의 전원을 끄지 않은 상태에서도 설치, 사용할 수 있는 핫도킹(Hot docking) 기능과 설치 후 바로 사용 할 수 있는 플러그 앤 플레이 기능 지원이 탁월해 컴퓨터에 주변기기를 부착할 때 가장 편리하게 연결할 수 있는 PC규격으로 평가받고 있다.

이러한 장점을 갖는 컴퓨터(2)에 내장된 USB 포트에, 도 2에 도시된 바와 같이, 종래 USB 포트 방식의 비밀키 저장장치(1)를 연결시킴으로써, 이 저장장치 에 미리 저장되어 있는 개인의 비밀키가 USB 포트를 통해서 컴퓨터에 고속 전송됨으로써, 컴퓨터를 재부팅 시키지 않고도 컴퓨터의 응용프로그램에 의해 비밀키를 사용 할 수 있게 하였다.

이러한 종래 USB 포트 방식의 비밀키 저장장치를 사용하여 도 3에 도시된 바와 같이 전자서명에 사용하려 할 때, 사용자는 컴퓨터에 설치된 전자서명 응용프로그램을 통하여 정식요구임을 승인하고 USB 포트 방식의 비밀키 저장장치 로부터 비밀키를 출력하고 계약서 등의 관련 데이터와, 컴퓨터에 설치된 전자서명 응용프로그램에서 비밀키(전자서명생성키)로 만든 전자서명, 자신의 전자서명 인증서를 모두 발송한다. 이 데이터를 접수한 전자서명 요구자는 이를 전자서명 검증키로 복호화 하여 암호화되지 않은 원본 데이터와 일치함을 확인함으로써 사용자의 신원 확인과 계약서 등의 관

련 자료가 위조되지 않았음을 확인한다.

그러나, 이러한 네트워크 환경에서 바이러스와 같이 사용자 모르게 설치된 해킹 프로그램은 그 비밀키를 해킹하여 다른 쇼핑몰에서 타인 명의로 물건을 구입할 수 있으므로, 본래 전자서명을 사용하는 사용자에게 피해를 입히는 경우가 자주 발생할 수 있다.

즉, 종래 USB 포트방식의 비밀키 저장장치의 경우는, 1회성이 아니라 컴퓨터의 USB 포트에 꽂아 둔 상태에 있었기 때문에 언제든지 혜커의 침입 혹은 컴퓨터의 사용자가 인식하지 못한 사이에 설치된 해킹 프로그램이 비정상적으로 USB 포트방식의 비밀키 저장장치로부터 비밀키를 요구하고 사용자의 승인을 무시하고 컴퓨터에 꽂아 둔 장치로부터 비밀키를 출력 받을 수 있어 문제점이 있었다. 이에 따라, 사용자의 비밀키를 보호하기 위한 가장 기본적인 방법으로는 비밀키 저장 장치 (스마트 카드, iKey 등) 등의 응용프로그램 제작 목적으로 프로그래머에게 배포되는 프로그래밍 라이브러리에 비밀키 저장장치로부터 비밀키를 발송하기 전에 사용자로 하여금 소프트웨어적인 확인 절차를 밟게 하는 방법이 있다. 그러나, 종래 USB 포트방식 혹은 스마트 카드 등의 비밀키 저장 장치로는, 각종 프로그램을 헤커들에 의한 소프트웨어적 비정상적 접근 즉, 컴퓨터 모니터 및 출력장치로 어떠한 출력도 보이지 않는 방법으로 비밀키 저장장치의 비밀키 출력을 시도하고 사용자의 인증을 실행한 것처럼 가장한 접근으로부터 그 효과를 기대할 수 없다.

또한, 사용자의 컴퓨터에 전자서명생성키 등의 비밀성이 유지되어야 하는 비밀키가 출력된다는 것은 정확하게 표현하여 사용자의 컴퓨터 메모리에 키 값이 로드(Load)된다는 것을 의미한다. 그러나, 전자서명생성키 등의 비밀성이 유지되어야 하는 비밀키가 컴퓨터의 메모리에 로드(Load) 된다는 것은 바이러스와 같이 자신도 모르게 자신의 컴퓨터에 설치되어 지는 많은 해킹 프로그램들이 사용자의 키보드 스트록(키보드 눌림 정보)과 컴퓨터 모니터 출력까지 가로 채고 있는 현재 해킹 기술상태에서 완벽한 안전성을 보장할 수 없다는 다른 문제점이 있다 (예를들어, 트로이의 목마, 백오리피스, PC ANYWAY 등).

전자서명은 누구나 전자서명의 내용을 확인 할 수 있기에 가능한 것이다. 그러나 특정 권한을 갖은 자에게만 자료가 공개되는 비밀성을 유지하는 데이터 또한 정보화시대에 반드시 필요한 사항이다. 이를 위하여 공개키 암호 시스템을 사용하는 방법으로 전자서명과 반대로 복호키를 비밀키로 가지고 있고 이 복호키로만 복호 할 수 있는 암호데이터 생성키 즉 암호키를 공개키로 배포하면 특정 권한자만 사용할 수 있는 데이터를 생성할 때는 해당 권한자의 공개된 암호키로 데이터를 암호화 하게되면 복호키를 알고 있는 권한자 만이 데이터를 복호해 사용할 수 있게 된다.

이와 같은 정보보호 방법은 소프트웨어적 비정상접근(해킹)을 방지하는 방법이다. 즉 비밀키를 저장한 장치를 사용 및 보관 미숙으로 인하여 분실 및 도난을 당한 경우 악성, 악의성 사용에 안전성을 보장 할 수 없다는 것이다. 이러한 물리적 접근 방지를 위하여 장치에 지문인식 기술을 도입하여 해당 사용자의 지문을 확인하여 사용한다면 분실 및 도난 등으로 인한 타인의 사용을 물리적으로 방지 할 수 있게 된다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명에서는 상기와 같은 종래 비밀키 저장장치를 컴퓨터에 꽂을 때 소프트웨어에 의한 비밀키가 출력되는 것으로 인해 발생되었던 소프트웨어적 비밀키 저장장치에 대한 해킹의 문제점(비정상적 요구에 의해 비밀키가 컴퓨터로 출력됨)을 해결하기 위해서 기계식 버튼 방식의 장치로 정보를 보호하고, 안전성의 확인이 되지 않는 컴퓨터의 메모리로 비밀키가 노출된다는 점으로 인해 발생되는 소프트웨어적 컴퓨터에 대한 해킹 방지를 위하여 암호/복호 기능을 내장한 장치로 비밀키의 출력이 없이 데이터의 입력과 암호화/복호화 데이터의 출력으로 비밀키를 보호하며, 비밀키 저장 및 암호/복호 장치를 사용자가 분실 혹은 도난 당하여 생기는 물리적 접근 방지 문제를 해결하기 위하여 지문인식에 의

한 장치의 작동으로 개인의 정보를 보다 안전하게 보장하는데 그 목적이 있다.

이와 같은 목적을 달성하기 위한 본 발명의 USB 포트방식의 비밀키 보안장치는 다음과 같다. 전원이 온(on)된 컴퓨터에 내장된 USB(Universal Serial Bus) 포트에 열쇠(Key)처럼 형태로 삽입된다. 먼저, 포트에 삽입됨과 동시에 전원 전송수단을 통해 컴퓨터로 부터 전원이 입력된다. 그 입력된 전원을 받은 전원 공급 및 차단수단은 사용자의 기계적인 조작에 의거하여 전원을 공급 및 차단 해준 다. 그리고, 지문인식수단은 전원 공급 및 차단 수단에서 공급된 전원으로 인에이 블 상태가 되고, 사용자의 지문을 스캐닝하여 그 스캐닝한 지문정보와 영구 메모리에 미리 저장된 지문정보가 일치할 때 암호 및 복호 선택수단을 사용 가능 상태로 만든다. 그리고 그 지문인식수단의 일치신호를 받은 후 사용가능 상태가 된 암호 및 복호 선택수단을 이용하여 사용자가 컴퓨터로 부터 입력되는 데이터를 암호 또는 복호로 선택한다. 또한, 데이터 입출력수단으로 USB 포트에 삽입되어, 전자서명에 필요한 원본 데이터 혹은 복호를 하기 위한 암호 데이터가 입력된다. 그리고 전원 공급 및 차단수단에서 공급된 전원으로 임시 메모리, 영구 메모리, 암호 및 복호 프로세서, 지문인식기가 인에이블 상태가 된다. 그리고, 임시 메모리에는, 원본데이터와 생성된 암호 및 복호 데이터가 임시 저장된다. 영구 메모리는, 비밀키(암호키 또는 복호키)와 사용자 지문정보가 미리 저장된다. 그리고 암호 및 복호 프로세서는, 암호 및 복호 선택수단의 선택에 따라 임시 메모리의 원본 데이터를 영구 메모리의 비밀키를 사용하여 암호화 또는 복호화하여 임시 메모리와 데이터 입출력수단을 통해 USB 포트에 출력시킨다.

이와 같은 본 발명은, 전원 공급 및 차단 수단의 기계적인 조작에 의해 소프트웨어적인 해킹 접근을 막을 수 있고, 비밀키를 본 비밀키 보안장치 외부로 출력하지 않고서도 전자서명을 할 수 있으며, 아울러, 보다 완벽하게 지문인식을 이용함으로써 분실 및 도난으로부터의 본 보안장치 도용을 방지할 수 있는 것이다.

발명의 구성 및 작용

이하, 본 발명을 첨부된 도면들에 의거하여 상세히 설명하면 다음과 같다.

정보화 시대, 특히 인터넷이 생활에 주요 통신 수단이 되고 있는 시대에 개인의 인증, 위조불가, 부인방지, 변경불가, 재사용불가, 비밀성 등과 같은 특성이 필요하다. 이를 위하여 전자서명과 데이터의 암호화를 하는 것이며, 절대적 필요사항은 전자서명생성키와 암호데이터 복호키의 비밀성에 있다.

정보 소유자의 요구대로 정보의 비밀을 유지하기 위해서 접근 통제 또는 개인 정보를 암호화하고, 정보를 주어진 권한에 의해서만(인가자에 의해서만) 변경 하기 위해서 물리적 통제 또는 접근 통제가 이루어져야 하며, 적절한 방법으로 컴퓨터 프로그램을 작동시키고 정당한 방법의 권한자의 서비스 요구시 거부하지 않도록 비밀성 유지, 물리적 위협 요소로부터의 보호가 각각 필요하다.

이와 같은 필요성에 따라 안출된 본 발명의 USB 포트 방식의 비밀키 보안장치의 제 1 실시예를 도 3에 도시된 바와 같이 구성할 수 있다. 이에 따른 그 구성을 살펴보면 다음과 같다.

전원을 온(ON) 시킨 컴퓨터(2)에 내장된 USB 포트(3)에 본 발명의 비밀키 보안장치(10)를 열쇠처럼 삽입한다. 이렇게 삽입되는 본 발명의 비밀키 보안장치 (10)의 구성은, 이 USB 비밀키 보안장치 삽입과 동시에 컴퓨터(2)로부터 공급되는 소정의 전원을 전송하는 전원전송단자(11)와, 전원전송단자(11)로부터 전송된 전원을 사용자의 기계적인 스위치의 온/오프 조작에 따라 공급 및 차단하는 전원 공급/차단 스위치(12)와, 전원 공급/차단 스위치(12)의 온(ON)조작에 의해 전원전송단자(11)로부터 전송된 전원을 입력받아 인에이블 상태로 되고, 미리 저장된 사용자의 비밀키 데이터를 출력하는 영구 메모리(ROM) (13)와, 그 영구 메모리(13)로부터 출력된 비밀키 데이터를 USB 포트(3)에 전송되게 하는 데이터 입출력 단자(14)로 구성된다. 상술한 비밀키 데이터는 이하에서도 마찬가지로, 정보통신부 장관 지정, 인증관리센터(한국정보보호센터)에서 관리하는 공인인증 기관에서 발급한 전자서명생성키 데이터 혹은 특정 단체에서 사용자인증 및 데이터의 비밀성을 유지하기 위해 특정 사용자에게만 배포된 비공개 키이다.

이와 같은 구성에 따른 동작을 살펴보면, 먼저 비밀키 보안장치 응용 프로그램으로부터의 비밀키 요구시 비밀키 보안장치(10)를 갖고 있는 사용자가 컴퓨터에 내장된 USB 포트(3)에 비밀키 보안장치(10)의 삽입부를 꽂는다. 이와 동시에, 전원전송단자(11)를 통해서 제공되는 전원을 사용자가 기계적인 스위치인 푸쉬 버튼이나 딥 스위치 등을 사용한 전원 공급/차단 스위치(12)를 온(ON) 시켜 전원을 영구 메모리(13)에 공급하여 인에이블 상태로 만들면서 그 영구 메모리(13)에 저장된 비밀키는 데이터 입출력단자(14)를 통해 USB 포트(3)에 전송후 디스에이블(disable) 상태가 되고, USB 포트(3)를 통해 비밀키를 입력받은 컴퓨터(2)는 비밀키 보안장치 응용프로그램에 의해 비밀 데이터(전자서명 등)를 생성 혹은 암호데이터를 복호하게 된다.

이와 같이 본 발명에서는 종래와 같이 비밀키 인증장치를 꽂으면 바로 컴퓨터에서 소프트웨어적으로 비밀키를 해당 장치에서 출력하여 비밀키를 사용하는 것이 아니라, 사용자의 기계적인 스위치의 조작으로 비밀키를 해당 장치에서 출력하여 사용함으로써, 컴퓨터에 연속적으로 연결되어 있는 장치에 소프트웨어적 비정상 접근을 차단하여 비밀키 출력에 대한 안전성을 보장받을 수 있다.

또한, 본 발명의 제 2 실시예를 도 4를 참조로 하여 설명하되, 사용자가 암호기능을 선택할 경우와 복호기능을 선택할 경우로 나누어서 구성 및 동작을 설명한다.(여기서의 암호/복호를 위한 구성은 동일하므로 동일부호를 사용한다). 상술 또는 후술할 전원 공급/차단 스위치는 푸쉬 버튼이나 딥 스위치 등을 사용하고, 또 영구 메모리는 ROM, EPROM 등을, 임시 메모리는 RAM을 사용하며, 아울러 암호/복호 선택 스위치는 딥 스위치 또는 푸쉬 버튼을 사용한다.

이에 먼저, 사용자가 암호기능을 선택할 경우의 제 2 실시예를 설명한다.

도 4에 도시된 본 발명의 USB 포트 방식의 비밀키 보안장치(20)의 구성을 살펴보면 다음과 같다.

전자서명 및 암호화에 사용할 경우 암호/복호 선택 스위치(21)를 암호에 맞추고 전원을 온 시킨 컴퓨터(2)에 내장된 USB 포트(3)에 본 발명의 보안장치(20)를 열쇠처럼 삽입한다. 이렇게 삽입되는 본 발명의 비밀키 보안장치(20)의 구성은, 사용자가 본 비밀키 보안장치 외부로 암호화한 데이터를 출력하기 위한 선택을 하는 암호/복호 선택 스위치(21)와, USB 비밀키 보안장치 삽입과 동시에 컴퓨터(2)로부터 공급되는 소정의 전원을 전송하는 전원전송단자(22)와, 전원전송 단자(22)를 통해서 전송되는 전원을 기계적인 온/오프 조작으로 공급 및 차단하는 전원 공급/차단 스위치(23)와, 스위치(23)의 조작으로 전원을 공급받으면 본 보안장치(20) 외부로부터 필요한 데이터(원본 데이터 또는 암호화할 데이터)를 입력받아 저장하고 암호/복호 프로세서(26)에서 생성된 암호 데이터를 저장하는 임시 메모리(24)와, 비밀키(암호키)가 미리 저장되어 있는 영구 메모리(25)와, 암호/복호 선택스위치(21)의 암호화 선택에 따라 영구메모리(25)의 비밀키(암호키)를 사용하여 임시 메모리(24)에 저장된 원본 데이터를 암호화 하는 암호/복호 프로세서(26)와, 이 프로세서(26)의 제어를 받아 그 임시 메모리(24)에 저장되는 암호 데이터를 USB 포트(3)로 출력하는 데이터 입출력 단자(27)로 구성된다.

이와 같은 구성에 의거한 동작을 살펴보면 다음과 같다. 먼저, 사용자가 암호/복호 선택 스위치(21)를 통하여 암호기능으로 선택하고 사용자가 본 발명의 비밀키 보안장치(20)를 USB 포트(3)에 삽입하면, 전원전송단자(22)를 통해 전원이 전송되고, 사용자가 푸쉬 버튼이나 딥 스위치(23) 등을 기계적으로 온(ON) 조작 하면 그때의 전원은 장치 내부의 임시메모리(24), 비밀키(암호키)가 저장되어 있는 영구메모리(25) 및 암호/복호 프로세서(26)에 공급되어, 본 발명의 비밀키 보안장치(20)는 사용가능상태가 된다. 이때의 전원 공급과 함께 ROM -BIOS가 저장된 영구 메모리(25)는 장치를 초기화하고 그와 동시에 데이터 입출력단자(27)를 통하여 전자서명에 필요한 원본 데이터가 임시메모리(24)에 로드 (Load)된다. 임시메모리(24)에 로드된 원본 데이터는 영구메모리(25)에 저장되어 있는 비밀키(암호키)로 암호/복호 프로세서(26)가 암호화하여 암호데이터를 생성한다. 그 생성된 암호 데이터를 암호/복호 프로세서(26)은 임시메모리(24)에 저장시킨다. 이에 따라 임시메모리(24)에 저장된 암호 데이터는 데이터 입출력단자(27)를 통하여 USB 포트(3)로 출력하게 된다.

이와 같이 본 발명에서는 종래와 같이 비밀성이 필요한 비밀키(암호키)를 장치 외부로 출력하여 컴퓨터의 프로세서와 메모리를 사용하는 응용 프로그램이 암호화를 하는 것이 아니라, 본 발명의 보안장치(20) 내부에서 원본 데이터가 장치 내부로 입력되어 생성된 암호 데이터를 출력하므로 비밀키(암호키)에 대한 비밀성 의 보장이 없는 컴퓨터에서도 비밀성을 보장받을 수 있게 된다.

상기와 마찬가지로, 도 4를 참조로 하여 본 발명의 비밀키 보안장치(20)에서 사용자가 복호기능을 선택할 경우에 따른 제 2 실시예를 설명한다.

이에 도시된 본 발명의 USB 포트 방식의 비밀키 보안장치(20)의 구성을 살펴보면 다음과 같다.

자신에게만 사용, 변경, 참조의 권한이 부여된 암호데이터를(공개되어 있는 자신의 암호키로 암호화된 데이터를) 복원하려 할 경우 암호/복호 선택 스위치를 복호로 선택하고 전원을 온 시킨 컴퓨터(2)에 내장된 USB 포트(3)에 본 발명의 USB 비밀키 보안장치(20)를 열쇠처럼 삽입한다. 이렇게 삽입되는 본 발명의 비밀키 보안장치(20)의 구성은, 사용자가 본 비밀키 보안장치 외부에서 암호화된 데이터를 입력받아 복호된 데이터로 출력하기 위한 기능 선택을 하는 암호/복호 선택 스위치(21)와, USB 비밀키 보안장치 삽입과 동시에 컴퓨터로부터 공급되는 소정의 전원을 전송하는 전원 전송단자(22)와, 전원전송단자(22)를 통해서 전송받은 전원을 사용자가 기계적인 조작으로 공급(ON)/차단(OFF)하는 전원 공급/차단 스위치(23)와, 이 스위치(23)의 공급(ON) 조작에 따라 본 장치 외부로부터 데이터 입출력단자(27)를 통해 암호화된 데이터를 입력받고, 암호화된 데이터가 임시 저장되는 임시메모리(24)와, 자신의 비밀키(복호키)가 저장되어 있는 영구메모리 (25), 영구메모리(25)의 비밀키(복호키)를 사용하여 임시 메모리(24)에 저장된 암호화된 데이터를 복호 하는 암호/복호 프로세서(26)와, 그 프로세서(26)의 연산 결과를 받아 임시 메모리(24)에 저장된 복호 데이터를 USB 포트(3)에 출력하는 데이터 입출력단자(27)로 구성된다.

이와 같은 구성에 따른 동작을 살펴보면, 외부로부터 입력되는 암호화된 데이터를 복호화하고자 할 경우 사용자가 암호/복호 선택스위치(21)를 이용하여 복호를 선택한 후 컴퓨터에 내장된 USB 포트(3)에 본 발명의 비밀키 보안장치 (20)를 꽂는다. 그리고 나서, 사용자가 전원전송단자(22)를 통해 입력되는 전원을 전원 공급/차단 스위치(23)를 온(ON) 시켜 장치 내부의 임시메모리(24), 영구메모리 (25), 암호/복호 프로세서(26)에 전원을 공급한다. 전원의 공급과 함께 영구메모리 (25)는 장치를 초기화하고 그와 동시에 데이터 입출력단자(27)를 통하여 암호 데이터가 임시메모리(24)에 임시 입력된다. 암호/복호 프로세서(26)는 영구메모리 (25)에 저장된 비밀키(복호키)를 사용하여 임시메모리(24)에 있는 암호 데이터를 복호하고 그 결과를 임시메모리(24)에 저장한다. 임시메모리(24)에 저장된 복호 데이터는 입출력단자(27)를 통하여 컴퓨터의 USB 포트(3)에 출력된다.

이와 같이 본 발명에서는 자신에게 권한이 부여된 암호 데이터를 복호화 함에 있어서 기존의 키보드, 스마트 카드, USB 비밀키 저장장치 등을 통해 비밀키(복호키)를 컴퓨터에 입력하는 방식과 달리, 암호 데이터를 비밀키 보안장치로 입력받아 비밀키(복호키)를 외부의 암호/복호 장치로 출력하지 않고 복호할 수 있게 된다. 이는 비밀성을 보장받지 못하는 컴퓨터의 사용에 있어서 자신의 비밀키(복호키)를 보호 할 수 있게 된다. 만약 악성, 악의성 프로그램이 설치되어있는 컴퓨터에서 암호 데이터를 복호함에 있어 기존의 방식을 사용할 경우 자신의 비밀키(복호키) 자체를 노출시킴으로 인하여 공개되어 있는 자신의 암호키로 암호화된 모든 데이터의 비밀성을 유지할 수 없게 되지만 본 비밀키 보안장치(20)를 사용할 때에는 복호된 하나의 데이터만 비밀성을 상실하여 보다 안전하고 연속적인 정보보안 효과를 제공할 수 있다.

또한, 본 발명의 제 3 실시예를 도 5에 도시하였다. 이에 도시된 본 발명의 USB 포트 방식의 비밀키 보안장치(30)는, 지문인식을 이용한 구성으로서, 그 구성 을 설명하면 다음과 같다.

전원을 온 시킨 컴퓨터(2)에 내장된 USB 포트(3)에 본 발명의 USB 포트 방식 의 비밀키 보안장치(30)를 열쇠처럼 삽입한다. 이렇게 삽입되는 본 발명의 비밀키 보안장치(30)의 구성은, USB 비밀키 보안장치 삽입과 동시에 컴퓨터로부터 공급되는 소정의 전원을 전송하는 전원전송단자(31)와, 전원전송단자(31)를 통해서 전송되는 전원을 사용자가 기계적인 조작으로 공급 및 차단하는 전원 공급/차단 스위치(32)와, 이 전원 공급/차단 스위치(32)를 전원 공급(ON)으로 조작시 장치를 초기화하고 비밀키(암호키, 복호키) 및 사용자 지문 정보가 저장되어 있는 영구 메모리(36)와, 사용자의 지문을 스캐닝하고, 그 스캐닝한 데이터가 영구 메모리(36)에 미리 저장된 사용자 지문 데이터와 일치하는지의 판단 결과에 따라 본 비밀키 보안장치의 작동 신호를 암호/복호 선택 스위치(34)에 출력하는 지문 인식기(33)와, 지문인식기(33)로부터 지문정보일치신호를 받아 인에이블 상태가 될 때, 사용자가 대상 데이터의 암호화 또는 복호화를 선택하기 위한 암호/복호 선택 스위치(34)와, 암호/복호 프로세서(37)에서 생성된 데이터(복호 데이터, 전자서명, 암호 데이터) 와 데이터 입출력단자(38)를 통해 외부로부터 입력된 입력 데이터(원본데이터 혹은 암호데이터)가 저장되는 임시메모리(35)와, 암호/복호 선택 스위치(34)의 선택신호에 따라 임시메모리(35)에 저장된 입력 데이터를 영구메모리(36)의 비밀키를 사용하여 암호 또는 복호하는 암호/복호 프로세서(37)와, 암호/복호 프로세서(37)가 생성한 결과물을 임시메모리(35)를 통해 USB 포트(3)에 출력하고 외부로부터 암호화된 데이터를 입력 받는 데이터 입출력단자(38)로 구성된다. 또한 상기한 구성에다가, USB 포트(3)로부터 공급되는 전원이 부족할 때를 대비하여 상기 전원전송단자(31)와 전원 공급 및 차단 스위치(32) 사이에, 소형 밧데리(예를들면, 손목시계 또는 전자수첩 등에 사용되는 수은 전지)를 삽설하거나, 어댑터(Adaptor)에 연결되어 전원이 공급되도록 전원 잭(jack) 삽입부를 더 설치한 실시예로도 구성할 수가 있다.

이와 같은 구성에 따른 동작을 살펴보면, 전원을 온(ON)시킨 컴퓨터에 내장된 USB 포트(3)에 본 발명의 비밀키 보안장치(30)를 꽂는다. 이에 따라, 전원전송단자(31)를 통해 입력되는 전원을 사용자가 전원 공급/차단 스위치(32)를 온(ON) 조작하여 장치 내부의 임시메모리(35), 영구메모리(36), 지문인식기(33), 암호/복호 프로세서(37)에 전원을 공급한다. 전원의 공급과 함께 영구메모리(36)는 장치를 초기화하고 지문인식기(33)는 스캐닝 대기상태가 된다. 사용자가 손가락을 지문인식기(33)에 올려놓으면 지문인식기는 스캐닝하여 그 스캐닝된 지문정보와 영구 메모리(36)에 미리 저장된 사용자 지문 정보를 비교한다. 이 비교 결과, 지문정보가 일치하면, 지문인식기(33)는 암호/복호 선택 스위치(34)를 인에이블 상태로 만들고 지문정보가 일치하지 않으면 디스에이블 상태로 만든다. 이때, 인에이블 상태인 암호/복호 선택 스위치(34)에서 사용자가 암호화 또는 복호화를 선택하면, 데이터 입출력단자(38)를 통하여 대상 데이터(암호화된 데이터 또는 암호화할 데이터)를 입력받아 임시 메모리(35)에 임시 저장한다. 그리고, 암호/복호 프로세서(37)는 그 암호 또는 복호 스위치의 선택에 따라 영구메모리(36)에 저장된 비밀키(암호키, 복호키)를 사용하여 임시메모리(35)에 저장되어 있는 대상 데이터를 암호화 또는 복호화하고, 그 결과를 임시메모리(35)에 저장한다. 이 임시메모리(35)에 저장된 암호 데이터 또는 복호 데이터는 데이터 입출력단자(38)를 통하여 컴퓨터의 USB 포트(3)에 출력과 함께 장치는 디스에이블 상태가 된다.

이와 같이 본 발명에서는 암호/복호를 선택하기 전에 지문인식기를 사용하여 한 번 더 물리적 인증절차를 수행함으로써, 사용자의 부주의로 인해 본 비밀키 보안장치(30)의 분실 및 고의적 도난 등의 물리적 접근봉쇄 불가능 상태가 되었을 경우, 타인이 본 비밀키 보안장치를 동작시킬 수가 없기 때문에 비밀키를 사용한 어떠한 연산 결과물을 생성할 수 없게 한다. 즉, 본 비밀키 보안장치를 이용하면 사용자의 관리 소홀로 발생되는 분실 및 도난으로부터도 사용자의 비밀성 유지 데이터를 안전하게 보호할 수 있게 된다. 이에 반해서, 종래 사용되었던 스마트 카드, 마그네틱 카드, USB 비밀키 저장 장치 등은 물리적 접근통제 불가능 상태에서 소프트웨어적인 비밀번호 입력 방식 등 을 사용하기 때문에 전문적인 기술이 없는 사람도 수 차례의 무작위 비밀번호 입력을 통하여 사용 가능할 뿐 아니라, 비밀번호 입력과정이 타인에게 노출되어 있기 때문에 물리적 접근 통제의 안전성을 보장받기 어려운 문제점이 있다.

발명의 효과

이상과 같은 본 발명은, 종래의 USB 포트 방식의 비밀키 저장장치에서와 같이 비밀성을 유지해야 하는 정보를 해킹의

우려가 많은 응용프로그램에 의해 저장장치 외부로 출력하여 정보보안을 유지할 수 없었던 문제점을, 본 발명의 출력 절차를 사용자의 기계적인 스위치 조작으로 사용자는 물리적 승인을 함으로 소프트웨어적인 USB 포트 방식의 비밀키 보안장치에 대한 해킹 접근으로부터 안전성을 강화하고, 비밀키(암호키, 복호키)의 장치 외부로의 출력 없이 해결하는 방법을 사용하여 소프트트웨어적인 해킹 접근으로부터 보다 안전성과 비밀성을 유지하는 효과를 얻을 수 있다.

또한, 지문인식 장치를 사용하여 사용자의 도난, 분실 등으로 인한 타인의 물리적 접근에 대하여 원래 사용자의 지문 없이는 사용 할 수 없도록 함으로써, 타인의 비밀키 도용을 방지할 수 있는 효과가 있다.

이러한 본 발명을 전자서명에 사용한다면 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하여 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진하는 효과가 있다.

(57) 청구의 범위

청구항 1.

전원이 온(on)된 컴퓨터에 내장된 USB(Universal Serial Bus) 포트에 키(Key) 형태로 삽입되되,

상기 포트에 삽입됨과 동시에 컴퓨터로부터 공급되는 전원이 전송되는 전원전송수단;

비밀키의 출력을 제어하기 위해 상기 전송된 전원을 사용자의 기계적인 조작에 따라 공급 또는 차단해주는 전원 공급 및 차단수단;

상기 조작에 따라 공급된 전원을 받아 인에이블 상태로 되면서 미리 저장되어 있는 전자서명에 필요한 컴퓨터 사용자의 비밀키 데이터를 출력하는 영구 메모리; 및

상기 포트에 삽입되어 상기 영구 메모리로부터 출력되는 비밀키 데이터를 상기 포트에 출력해주는 데이터 입출력 수단으로 구성되어, 본 장치에 대한 타인의 소프트웨어적인 해킹 접근으로 정보 누출을 방지할 수 있는 것을 특징으로 하는 USB 포트 방식 의 비밀키 보안장치.

청구항 2.

제 1 항에 있어서, 상기 전원 공급 및 차단 수단은,

푸쉬 버튼 또는 딥 스위치를 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 3.

제 1 항에 있어서, 상기 영구 메모리는 ROM 또는 EPROM을 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 4.

전원이 온(on)된 컴퓨터에 내장된 USB(Universal Serial Bus) 포트에 키(Key) 형태로 삽입되되,

사용자가 상기 컴퓨터로부터 입력되는 입력 데이터(암호화할 데이터 또는 복호화할 데이터)를 암호화 또는 복호화로 선택하기 위한 암호 및 복호 선택수단;

상기 포트에 삽입됨과 동시에 컴퓨터로부터 공급되는 전원이 전송되는 전원전송수단;

상기 전송된 전원을 사용자의 기계적인 조작에 따라 공급 또는 차단해주는 전원 공급 및 차단수단;

상기 포트에 삽입되어, 암호화 할 원본 또는 복호하기 위한 데이터가 입력되고 암호 또는 복호화 된 데이터가 출력되는 데이터 입출력수단;

상기 전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고 상기 데이터 입출력수단을 통해 입력된 데이터와 프로세서에서 처리된 암호 또는 복호화 된 데이터가 임시 저장되는 임시 메모리;

상기 전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고 비밀키(암호키 또는 복호키)가 미리 저장되어 있는 영구 메모리; 및

상기 전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고 상기 암호 및 복호 선택수단의 선택에 따라 상기 임시 메모리의 데이터를 상기 영구 메모리의 비밀키를 사용하여 암호화 또는 복호화하여 상기 임시 메모리와 상기 데이터 입출력수단을 통해 상기 포트에 출력시키는 공개키 암호화 시스템 기반의 암호 및 복호 프로세서로 구성되어, 본 장치 외부로의 비밀키 출력없이 안전성과 비밀성 을 유지할 수 있는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 5.

제 4 항에 있어서, 상기 전원 공급 및 차단 수단은,

푸쉬 버튼 또는 딥 스위치를 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 6.

제 4 항에 있어서, 상기 영구 메모리는 ROM 또는 EPROM을 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 7.

제 4 항에 있어서, 상기 임시 메모리는 RAM을 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 8.

제 4 항에 있어서, 상기 암호 및 복호 선택수단은, 푸쉬 버튼 또는 딥 스위치를 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 9.

전원이 온(on)된 컴퓨터에 내장된 USB(Universal Serial Bus) 포트에 키(Key) 형태로 삽입되되,

전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고, 사용자의 지문을 스캐닝하여 그 스캐닝한 지문정보와 영구 메모리에 미리 저장된 지문정보가 일치할 때 암호 및 복호 선택수단을 사용가능상태로 만드는 지문인식 수단;

상기 지문인식수단의 일치신호를 받은 후 사용자가 상기 컴퓨터로부터 입력되는 데이터를 암호 또는 복호로 선택하기 위한 암호 및 복호 선택수단;

상기 포트에 삽입됨과 동시에 컴퓨터로부터 공급되는 전원이 전송되는 전원전송수단;

상기 전송된 전원을 사용자의 기계적인 조작에 따라 공급 및 차단해주는 전원 공급 및 차단수단;

상기 포트에 삽입되어, 전자서명에 필요한 암호화할 또는 암호화된 데이터가 가 입력되고 암호 또는 복호화 된 데이터가 출력되는 데이터 입출력수단;

상기 전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고 암호화할 또는 암호화된 데이터와 프로세서에서 처리된 암호 또는 복호 데이터가 임시 저장되는 임시 메모리;

상기 전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고 비밀키(암호키 또는 복호키)와 사용자 지문정보가 미리 저장되어 있는 영구 메모리;

상기 전원 공급 및 차단수단에서 공급된 전원으로 인에이블 상태가 되고 상기 암호 및 복호 선택수단의 선택에 따라 상기 임시 메모리의 데이터를 상기 영구 메모리의 비밀키를 사용하여 암호화 또는 복호화 하여 상기 임시 메모리와 상기 데이터 입출력수단을 통해 상기 포트에 출력시키는 공개키 암호화 시스템 기반의 암호 및 복호 프로세서로 구성되어, 사용자의 분실이나 도난으로 인해 타인이 도용하는 것을 방지할 수 있는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 10.

제 9 항에 있어서, 상기 전원 공급 및 차단 수단은,

푸쉬 버튼 또는 딥 스위치를 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 11.

제 9 항에 있어서, 상기 영구 메모리는 ROM 또는 EPROM을 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 12.

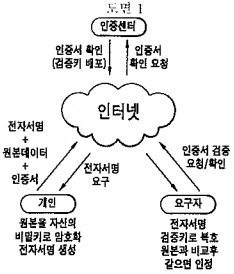
제 9 항에 있어서, 상기 임시 메모리는 RAM을 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

청구항 13.

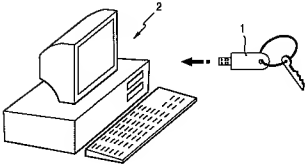
제 9 항에 있어서, 상기 암호 및 복호 선택수단은, 푸쉬 버튼 또는 딥 스위치를 사용하는 것을 특징으로 하는 USB 포트 방식의 비밀키 보안장치.

도면

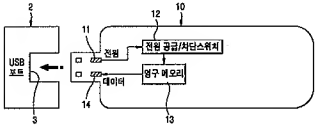
도면 1



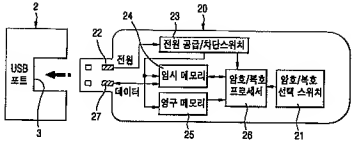
도면 2



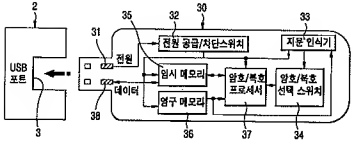
도면 3



도면 4


2
24
23
20
22
전원 공급/차단스위치
USB 포트
전원
임시 메모리
암호/복호 프로세서
암호/복호 선택 스위치
데이터
영구 메모리
27
3
25
26
21

도면 5


2
35
32
30
33
31
전원 공급/차단스위치
지문 인식기
USB 포트
전원
임시 메모리
암호/복호 프로세서
암호/복호 선택 스위치
데이터
영구 메모리
38
3
36
37
34